CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

Sub A2

~~1. A method for communication between two entities in a set of clients across a network such that their identities are concealed from each other and no third party is able to trace the communication comprising the steps of:~~

~~providing a set of Forwarding Agents (FAs), there being *n* FAs and several groups of these *n* agents, each of which consists of *k* members, where *k* $(0 < k \leq n)$ is a fixed number considered sufficient to provide anonymity in the system and each FA belongs to at least one group;~~

~~providing each of the FAs with its own pair of public and private keys for encryption and decryption, respectively, where the underlying cryptosystem scheme is a commutative public key cryptosystem, each FA also having appropriate keys required to perform secure digital signatures on documents and to verify the signatures of other FAs;~~

~~registering each client with a Forwarding Agent S, the client once having selected a Forwarding Agent S, also picking one of the groups that the Forwarding Agent S belongs to, thus selecting *k* agents to be associated with the client, the step of registering including assigning a pseudonym X to the client and providing the Forwarding Agent S with an encrypted form of the client's network address, rendering it unreadable to any individual FA;~~

~~maintaining by each FA a table with three fields, a pseudonym, a corresponding encrypted network address and the FA group to be used for forwarding;~~

~~delivering a message meant for a pseudonym X to Forwarding Agent (FA) S where X is registered using a protocol that protects the anonymity of~~

the sender;

passing the message through a random sequence of FAs in the group to which Forwarding Agent S belongs; and

finding by the last FA in the sequence a visible network address and sending the message on to this address.

a2

2. The method for communication recited in claim 1, wherein the step of registering comprises the steps of:

successively encrypting by the client the client's network address with the public keys of the *k* selected agents to obtain an encrypted address, referred to as the "onion address" of the client;

sending by the client to the Forwarding Agent (FA) S a Registration Message which contains the client's onion address and a chosen pseudonym X, and also identifies the group of *k* agents selected by the client; and

adding by the Forwarding Agent the information contained in the Registration Message to its table.

3. The method for communication recited in claim 2, wherein the Registration Message is sent using a protocol which protects the anonymity of the sender.

4. The method for communication recited in claim 3, wherein the protocol used comprises the Forwarding Agent (FA) S having a publicized pseudonym and the client sending a message to that pseudonym.

5. The method for communication recited in claim 1, wherein once the Forwarding Agent (FA) S obtains a message intended for X, the Forwarding Agent S performs the steps of:

looking up X in its internal table and retrieving an encrypted version of the address of X, referred to as the "onion address" of X, as well as the group of FAs to be used for forwarding;

creating the list of the FAs that the message will pass through, which list includes all FAs other than Ṡ who will have to "peel the onion" before the address of the intended recipient is revealed, the list containing all the members of the appropriate group except the Forwarding Agent S itself; and

affixing the list to the head of the message.

a2

6. The method of communication recited in claim 5, further comprising the step of encrypting the message before forwarding it to FAs in the sequence.

7. The method of communication recited in claim 6, wherein the step of encrypting comprises the steps of:

splitting the message into blocks of a fixed size;

prefixing each block with a fixed number of random bits, producing blocks of a larger size; and

encrypting each block of a larger size with the public key or shared symmetric key of the intended recipient.

8. The method of communication recited in claim 6, wherein each FA which receives the message performs some verifications to ensure protocol consistency by other FAs.

9. The method of communication recited in claim 8, wherein the verifications comprise the steps of:

checking by an agent whether it is the first agent to be visited in the current domain and, if so, selecting at random a tag N which has not been recently used and affixing the tag to the message header before passing the message on;

otherwise, finding out the name S of the first agent to receive this message in the current domain;

verifying a signature of S on a first part of the signed sequence in the message header and, if this verification succeeds, then verifying that every successive segment of the signed sequence bears the valid signature of the agent named in the preceding segment;

verifying that the last segment of the signed sequence contains the name of the agent performing the verification, while the penultimate segment contains the name of the agent from which the message was received;

verifying that the list of unvisited agents does not contain any agents named in the signed sequence; and

if any of the verifications fail, aborting the current message.

10. The method of communication recited in claim 8, wherein the verifications comprise the steps of:

computing the agent's own sequence number *i* in the path followed by this message through the set of forwarding agents by subtracting the number of FAs in the list of unvisited FAs from $k + 1$;

checking if *i* is 1 and, if *i* is 1, then sending a coordinating agent (CA) 0 a request for a tag and receiving the tag N as well as the number $k - 1$, combined with N and signed before passing the message on;

if the number *i* is found to be different from 1, then verifying the signature of CA $(i - 2)$ mod *r* on the signed number in the message header and, if verification succeeds, then verifying if the signed number is $k + 1 - i$ and, if the verification succeeds, sending the numbers $k + 1 - i$ and N and the name of the previous FA to CA $(i - 1)$ mod *r;*

receiving a signed number and a signal from CA $(i - 1)$ mod *r* and verifying if the signal is "OK" and, if so, verification is complete and the message is passed on; but

if any of the verifications fail, concluding that the protocol has not been executed correctly and aborting the current message.

11. The method of communication recited in claim 10, wherein the CA, upon receiving a request from some FA, referred to as P, for a tag, performs the steps of:

selecting a tag N and sending it to P;

combining the tag N with a number $k - j$, signing the result and sending the signed number to P along with an "OK" signal;

waiting for a message about the tag N, and upon receiving such a message, verifying if it came from the next CA referred to as D, and if the message did not come from D, announcing a protocol violation in receiving tag N;

otherwise, verifying the message involves the number $k - 1$, and if this verification fails, sending an "Abort" message to D; but

if the verification passes, sending to D an "OK" signal and the identity of P.

12. The method of communication recited in claim 10, wherein any CA other than CA 0, upon receiving a message from some FA referred to as P, performs the steps of:

finding a number j, a tag N, and the identity of P, the previous FA, in the message;

sending a message to the previous CA asking for the name of the corresponding FA, for tag N, and number $j + 1$;

receiving a signal and a table from the previous CA, and verifying that the signal is "OK" and the name is P, and if such verification fails, sending an "Abort" signal to P;

otherwise, verifying that the most recent request, if any, involving the tag N involved the number $j+1$, verifying that it is the $(k-j)^{\text{th}}$ CA, and if either of these verifications fails, sending an "Abort" signal to P;

but if the verifications pass, combining $j-1$ with N, signing the result and sending the signed number to P along with an "OK" signal;

waiting for a message about the tag N, and upon receiving such a message, verifying if it came from the next CA referred to as D, and if the message did not come from D, announcing a protocol violation in writing tag N;

otherwise, verifying the message involves the number $j-1$, and if this verification fails, sending to D an "OK" signal and the identity of P.

a2

13. The method of communication recited in claim 5, wherein a next FA is chosen comprising the steps of:

checking by an agent if there are any more agents to be visited in the present domain and, if not, then marking the present domain as visited and removing the signed sequence from the message header;

choosing an unvisited domain at random and making it the present domain;

choosing an agent belonging to the current domain at random from the list of unvisited agents and, following this, passing the message on to the chosen agent;

if, instead, the agent finds that not all the agents in the domain have been visited, then choosing at random an unvisited agent belonging to the current domain;

combining the random number N with the name of the chosen agent

~~and signing the resulting plaintext; and~~

~~adding the plaintext and signature to the signed sequence, following which the message is forwarded to the chosen agent.~~

a2

~~14. The method of communication recited in claim 5, wherein a next FA is chosen comprising the steps of:~~

~~choosing by a current forwarding agent an FA at random from the list of unvisited FAs in the message header;~~

~~removing its own name from the list;~~

~~adding the signed number that it received from an appropriate coordinating agent (CA) to the message header; and~~

~~forwarding the message to the next chosen agent.~~